Available online at www.sciencedirect.com

SCIENCE DIRECT®

Finite Fields and Their Applications 9 (2003) 395–399

FINITE FIELDS AND THEIR APPLICATIONS

http://www.elsevier.com/locate/ffa

The extremal codes of lengths 76 with an automorphism of order 19 ☆

Radinka Dontcheva[a,1] and Vassil Yorgov[b,*]

[a] *Faculty of Information Technology and Systems, Delft University of Technology, 2628 CD Delft, The Netherlands*

[b] *Department of Mathematics and Computer Science, Fayetteville State University, Fayetteville, NC 28301, USA*

Received 10 March 2002; revised 29 January 2003; accepted 13 February 2003

Communicated by Vera Pless

Abstract

We find all extremal [76,38,14] binary self-dual codes having automorphism of order 19. There are three inequivalent such codes. One of them was previously known. The other two are new. These codes are the shortest known self-dual codes of minimal weight 14 as well as the best-known linear codes of that length and dimension.

Keywords: Extremal self-dual codes; Automorphisms; Optimal codes

1. Introduction

It is known [3] that the weight enumerator, W, of an extremal binary [76,38,14] self-dual code and the weight enumerator, S, of its shadow have one of the forms

$$W = 1 + (4750 - 16\alpha)y^{14} + (79895 + 64\alpha)y^{16} + (915800 - 64\alpha)y^{18} + \cdots$$

$$S = \alpha y^{10} + (9500 - 14\alpha)y^{14} + (1831600 + 91\alpha)y^{18} + (105689400 - 364\alpha)y^{22} + \cdots, \quad (1)$$

☆ This work was partially supported by project 5/8.5.2001 of Shoumen University.

* Corresponding author. Tel.: 910-672-1675; fax: 910-672-1675.

E-mail addresses: r.a.doncheva@its.tudelft.nl (R. Dontcheva), vyorgov@uncfsu.edu (V. Yorgov).

[1] On leave from Shoumen University, Shoumen 9712, Bulgaria.

1071-5797/03/$ - see front matter
doi:10.1016/S1071-5797(03)00012-1

where $0 \leqslant \alpha \leqslant 296$,

$$W = 1 + 2590y^{14} + 106967y^{16} + 674584y^{18} + \cdots$$

$$S = y^2 + 8954y^{14} + 1836865y^{18} + 105664452y^{22} + \cdots \tag{2}$$

or

$$W = 1 + (4750 + 16\alpha)y^{14} + (80919 - 64\alpha)y^{16} + (905560 - 64\alpha)y^{18} + \cdots$$

$$S = y^6 + (-16 - \alpha)y^{10} + (9620 + 14\alpha)y^{14} + (1831040 - 91\alpha)y^{18} + \cdots, \tag{3}$$

where $-296 \leqslant \alpha \leqslant -16$.

In [1] a code is obtained with weight enumerators W and S of form (1) with $\alpha = 0$. That code has an automorphism of order 19. In this work we use a field of 2^{18} elements to find all [76,38,14] codes having an automorphism of order 19. There are three inequivalent such codes. All of them have the same weight enumerator (namely (1) with $\alpha = 0$) and are shadow extremal (see [3,4]). As can be seen in [3], a self-dual binary code with minimum distance 14 can exist for some smaller lengths (74, 72, and 70). No such codes are known. These codes have the largest minimum distance among the all known linear codes of length 76 and dimension 38 (see [2]).

2. The code construction

We use the method developed in [6–8]. Until the end of the work C will denote a [76,38] self-dual code.

Lemma 1. *If C has minimum weight* 14 *and an automorphism, σ, of order* 19 *then there are* 4 *cycles of length* 19 *in the cycle decomposition of σ.*

This lemma follows from Theorem 1 and Corollary 4 of [7].

From now on we assume that C is a code of minimum weight 14 that has an automorphism

$$\sigma = (1, 2, \ldots, 19)(20, 21, \ldots, 38)(39, 40, \ldots, 57)(58, 59, \ldots, 76).$$

Denote $F_\sigma(C) = \{v \in C \mid v\sigma = v\}$. Let $E_\sigma(C)$ be the set of all vectors in C having even weight on each cycle of σ. The code C can be decomposed as a direct sum of $F_\sigma(C)$ and $E_\sigma(C)$ [6]. Let $GF(2)$ be the binary field and let $\pi : F_\sigma(C) \to GF(2)^4$ be the "contraction" map which deletes all but one of the coordinates of $v \in F_\sigma(C)$ in every cycle of σ. Then $\pi(F_\sigma(C))$ is a self-dual $[4, 2]$ binary code. Hence we can assume that $\pi(F_\sigma(C))$ is generated by the matrix

$$\begin{pmatrix} 1 & 1 & 0 & 0 \\ 0 & 0 & 1 & 1 \end{pmatrix}.$$

This determines the last two rows of the generator matrices in Theorem 1. Let P be the binary cyclic code of length 19 generated by $x-1$. Since the parity check polynomial $\frac{x^{19}-1}{x-1}$ is irreducible over the field $GF(2)$, P is a field with 2^{18} elements.

Every restriction of a vector of $E_\sigma(C)$ on a cycle of σ has even weight and can be viewed as an element of P. Denote by $\varphi(E_\sigma(C))$ the image of $E_\sigma(C)$ under this identification.

It follows from Theorem 2 of [7] that $\varphi(E_\sigma(C))$ is a self-dual $[4,2]$ code over the field P with respect to the following inner product:

$$u_1v_1^{2^9}+u_2v_2^{2^9}+u_3v_3^{2^9}+u_4v_4^{2^9}=0. \tag{4}$$

If there is a weight 2 vector in $\varphi(E_\sigma(C))$ it will generate a [38,18,14] binary code. The Griesmer bound [5] implies that such a code does not exist. Thus $\varphi(E_\sigma(C))$ is a [4,2,3] maximum distance separable (MDS) code over the field P and any two coordinates are information positions.

The next lemma follows immediately from Theorem 3 of [8].

Lemma 2. *Two* [76,38,14] *self-dual codes C and C' having automorphism σ are equivalent iff the code C' can be obtained from the code C applying a product of some of the following transformations*:

(i) *The substitution $x\to x^2$ in $\varphi(E_\sigma(C))$;*
(ii) *A multiplication of the jth coordinate of $\varphi(E_\sigma(C))$ by x^{t_j}, where t_j is a nonnegative integer, $j=1,2,3,4$;*
(iii) *A permutation of the four cycles of C.*

Let e be the identity of P, $\alpha=x+x^2+x^5+x^6+x^{13}+x^{14}+x^{17}+x^{18}$, and $b=x^4+x^7+x^8+x^9+x^{10}+x^{11}+x^{12}+x^{15}+x^{16}+x^{17}$. The multiplicative orders of α, b, and xb in the field P are 2^9-1, $(2^9+1)/19$, and 2^9+1, respectively.

The next lemma follows from Lemma 2 and the self-duality of $\varphi(E_\sigma(C))$.

Lemma 3. *There is a generator matrix of $\varphi(E_\sigma(C))$ of the form*

$$\begin{pmatrix} e & 0 & \alpha^i b^{s_1} & \alpha^j b^{s_2} \\ 0 & b^{s_3} & \alpha^j b^{s_1} & \alpha^i b^{s_2} \end{pmatrix},$$

where $\alpha^i+\alpha^j=e$, $1\leqslant i\leqslant 510$, $1\leqslant j\leqslant 510$, $i<j$, and $0\leqslant s_t\leqslant 26$ for $t=1,2,3$.

An application of transformation (i) of Lemma 2 results in multiplication by 2 (mod 511) of the numbers i and j of Lemma 3. Using a computer we find representatives of the orbits under multiplication by 2 (mod 511) of all pairs (i,j) satisfying the conditions of Lemma 3. These representatives are $(1,93)$, $(6,13)$, $(7,505)$ $(9,59)$, $(15,37)$, $(19,105)$, $(20,99)$, $(21,87)$, $(25,251)$, $(29,178)$, $(31,193)$,

$(34,175)$, $(39,111)$, $(43,246)$, $(45,61)$, $(46,255)$, $(49,119)$, $(63,190)$, $(73,219)$, $(83,138)$, $(91,167)$, $(94,169)$, $(103,108)$, $(106,239)$, $(114,221)$, $(125,187)$, $(155,213)$, $(179,220)$, $(191,242)$.

Each permutation of the code cycles with $(1,3)(2,4)$, $(1,2)(3,4)$ and the nine-fold application of the first transformation of Lemma 2 leave the numbers i and j unchanged and transforms the triples (s_1,s_2,s_3) according to the rules $(s_1,s_2,s_3)\to(-s_1,s_3-s_1,s_2-s_1) \pmod{27}$, $(s_1,s_2,s_3)\to(s_2-s_3,s_1-s_3,-s_3) \pmod{27}$, and $(s_1,s_2,s_3)\to(-s_1,-s_2,-s_3) \pmod{27}$, respectively. The above three rules split the set of all triples (s_1,s_2,s_3) of Lemma 3 on 2744 orbits. For each of the 29 choices for $\{i,j\}$ determined above and for each representative (s_1,s_2,s_3) of the 2744 orbits, a generator matrix of a binary [76,38] code was obtained and the code was tested with a computer for nonzero vectors of weight less than 14. Only three extremal codes C_1, C_2, C_3 were found. The corresponding values of the parameters are given in Table 1.

It follows from Lemma 2 that these three codes are inequivalent. Just to be on the safer side we computed for each code the numbers Min and Max given in the last two columns of the table. These numbers are invariants for equivalent codes. Let A_{lt} be the number of codewords of weight 14 that cover coordinate positions l and t. Then Min (Max) is the smallest (largest) of the numbers $\{A_{lt} \mid 1\leqslant l<t\leqslant 76\}$.

Thus we have the following theorem. To save space some vectors are given in *hexadecimal*, using $0=0000$, $1=0001$, …, $9=1001$, $A=1010$, …, $F=1111$. The vectors are right-justified and the leading zeros are omitted.

Theorem 1. *There are exactly three inequivalent* [76,38,14] *binary self-dual codes*, C_1, C_2, *and* C_3, *with automorphism of order* 19. *A generator matrix for* C_i, $i=1,2,3$, *is*

$$\begin{pmatrix} V_1^{(i)} & 0 & V_2^{(i)} & V_3^{(i)} \\ 0 & V_4^{(i)} & V_5^{(i)} & V_6^{(i)} \\ J & J & 0 & 0 \\ 0 & 0 & J & J \end{pmatrix},$$

where the cells $V_j^{(i)}$, $1\leqslant i\leqslant 3$, $1\leqslant j\leqslant 6$ *are* 18×19 *circulant type matrices and* J *is the* 1×19 *all one matrix. The first rows of the matrices* $V_j^{(i)}$ *are given in Table 2. These three codes have weight enumerators* W *and* S *of the form* (1) *with* $\alpha=0$.

The code C_1 was first found in [1].

Table 1
Code parameters

Code	(i,j)	(s_1,s_2,s_3)	Min	Max
C_1	$(1,93)$	$(1,13,17)$	127	183
C_2	$(45,61)$	$(14,24,16)$	127	185
C_3	$(46,255)$	$(5,25,19)$	129	179

Table 2
First rows

Code	$V_1^{(i)}$	$V_2^{(i)}$	$V_3^{(i)}$	$V_4^{(i)}$	$V_5^{(i)}$	$V_6^{(i)}$
C_1	3*FFFF*	5*DDB*2	6*D*8*C*5	317*B*1	5927*C*	5*A*87*F*
C_2	3*FFFF*	43155	3655*A*	13*ED*2	5456*E*	13*FDA*
C_3	3*FFFF*	24*B*7	41*BCD*	2786*D*	*C*7*EA*	6*EF*58

Acknowledgments

The authors are grateful to the anonymous referee for the useful suggestions. The first author is thankful to Delft University of Technology for the excellent working conditions provided.

References

[1] A. Baartmans, V. Yorgov, Some new extremal codes of lengths 76 and 78, IEEE Trans. Inform. Theory 45 (2003), to appear.
[2] A.E. Brouwer, Bounds of the size of linear codes, in: V. Pless, W.C. Huffman (Eds.), Handbook of Coding Theory, Elsevier, Amsterdam, The Netherlands, 1997 8:ISBN: 0-444-50088-X. Available online: http://www.win.tue.nl/~aeb/voorlincod.html.
[3] S.T. Dougherty, T. Aaron Gulliver, M. Harada, Extremal binary self-dual codes, IEEE Trans. Inform. Theory 43 (1997) 2036–2047.
[4] S.T. Dougherty, M. Harada, Shadow optimal self-dual codes, Kyushu J. Math. 53 (1999) 223–237.
[5] J.H. Griesmer, A bound for error-correcting codes, IBM J. Res. Dev. 4 (1960) 532–542.
[6] W.C. Huffman, Automorphisms of codes with applications to extremal doubly-even codes of length 48, IEEE Trans. Inform. Theory 28 (1982) 511–521.
[7] V.Y. Yorgov, Binary self-dual codes with automorphisms of odd order, Probab. Pered. Inform. 19 (1983) 11–24 (in Russian).
[8] V.Y. Yorgov, A method for constructing inequivalent self-dual codes with applications to length 56, IEEE Trans. Inform. Theory 33 (1987) 77–82.